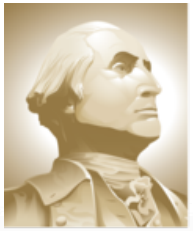


THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

CAAREN
Capital Area Advanced Research and Education Network | Powered by GW

Capital Region Advanced Cyber Range (CRACR)

Smart Cities • IoT • Industrial Control Systems
(Cybersecurity Education Focus)

Advanced Facility for Cybersecurity Education
a Platform for Training, Research and Experimentation

CICI: Regional: Substrate for Cybersecurity Education; a Platform for Training, Research and Experimentation (**SCEPTRE**)
a project sponsored by The National Science Foundation (Award #1642118)

Cyber Range

A well-defined, controlled environment

- Security
- Protocols
- Targets
- Weapons
- Events

weapons training • calibration • testing • offense • defense

… *just like a (military) shooting range*

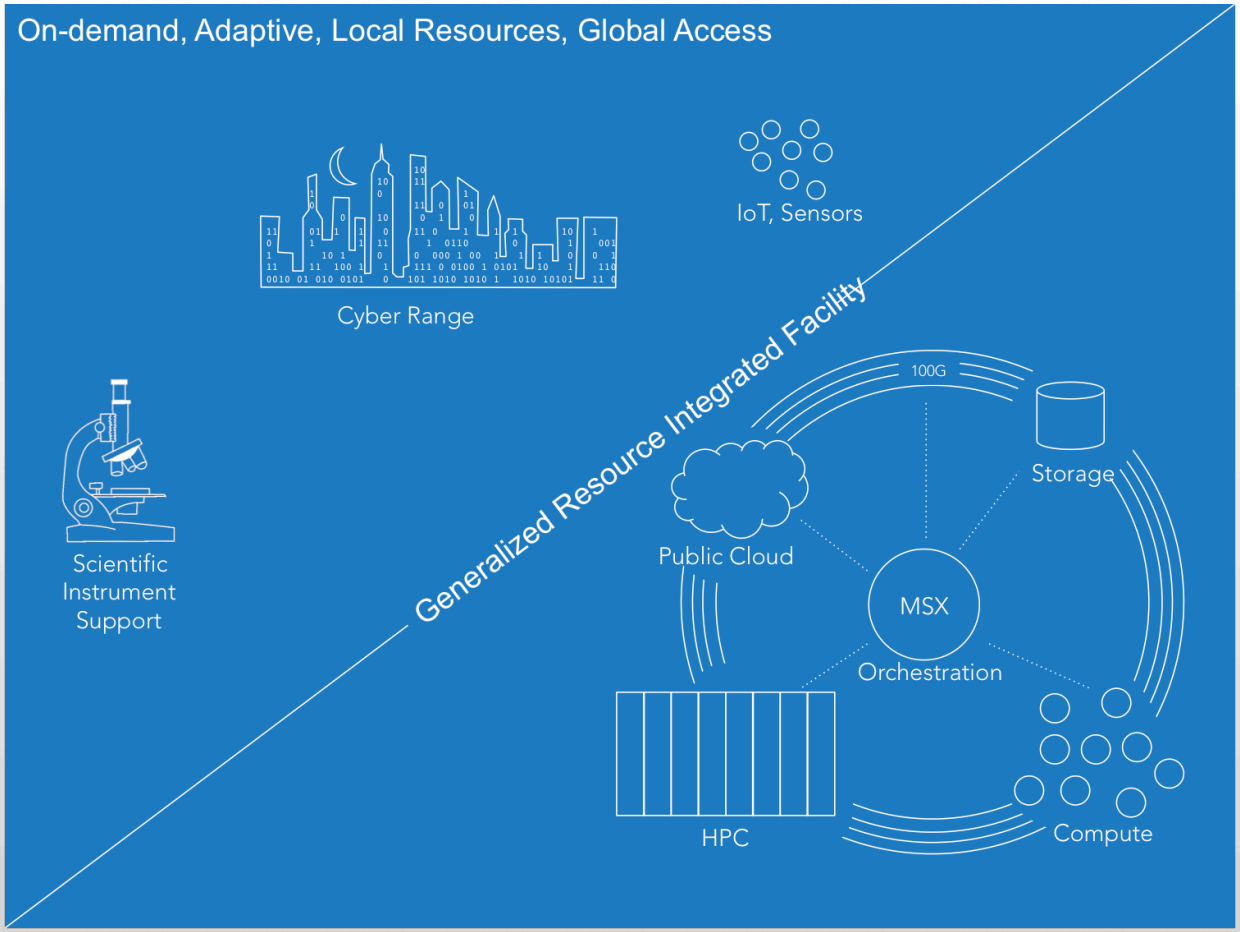
Cyber Infrastructures

- Virtualizable
  - *e.g.* power plant cyberinfrastructure systems (Engineering Workstations, DBs, Mail Servers, Network Elements, *etc.*)
- Hard or Impossible to Virtualize
  - Sensors, IoT, Actuators, PLCs, *etc.* (things with physical inputs, electro-mechanical properties and/or non-standard implementations (FPGAs, DSPs) or communication protocols (Modbus, Profinet, …))

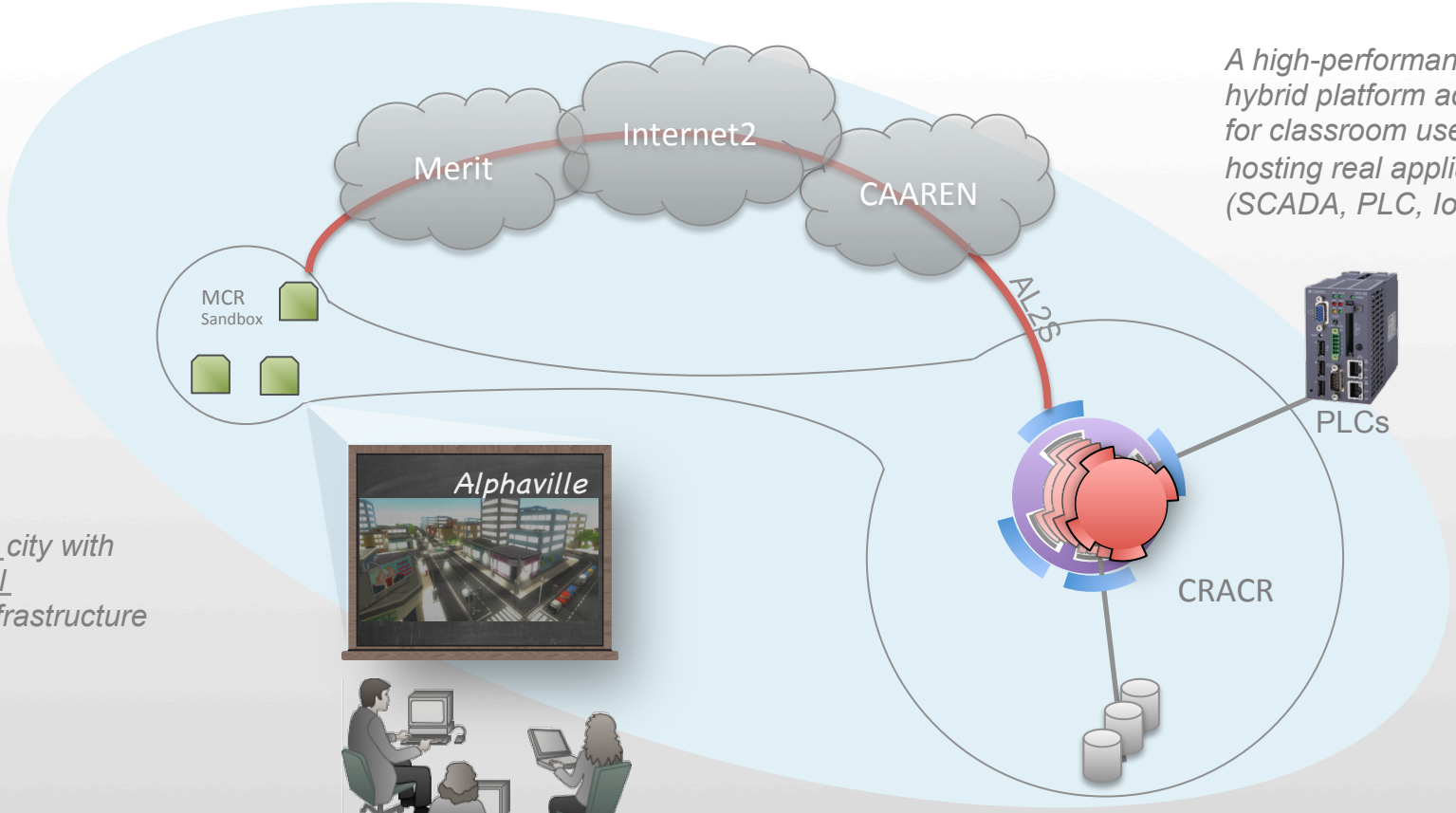
… there is an advantage in having a physically accessible Virtual Machine

Foundation: Open Science Platform

- Powerful
- Adaptable
- Versatile
- Scalable



Open Science Platform Application: Cyber Range



A high-performance, hybrid platform adapted for classroom use hosting real appliances (SCADA, PLC, IoT)

A virtual city with very real Cyberinfrastructure

The George Washington University

- College of Professional Studies
  - Principles of Cybersecurity
  - Ethics, Law & Policy
  - Compliance & Risk Management
  - IP Security & VPN Technology
  - Incident Response
  - Network Security
  - Securing Operating Systems
  - IT Security System Audits
  - Intrusion Detection & Vulnerability Management
  - IT Security Defense Countermeasures
  - Cyber Investigation
  - **Attacker Tools & Techniques**
  - Digital Forensics
  - Project Management for IT

Current Active Courses

College of
Professional Studies

THE GEORGE WASHINGTON UNIVERSITY

B.S.P.S. in Cybersecurity

Semester/Year **Spring 2018**

Course Name **Attack Tools & Techniques**

Course Number **PSCS 420**

Credits **4**

Program Learning Objectives

- Understand and implement Cybersecurity requirements;
- Investigate and analyze Cybersecurity incidents;
- Protect and effectively defend computer networks against malicious activities;
- Identify and correct computer network vulnerabilities through penetration testing and hacking techniques;
- Initiate and undertake critical analysis of security issues to develop and implement security policies and to solve problems;
- Interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals.

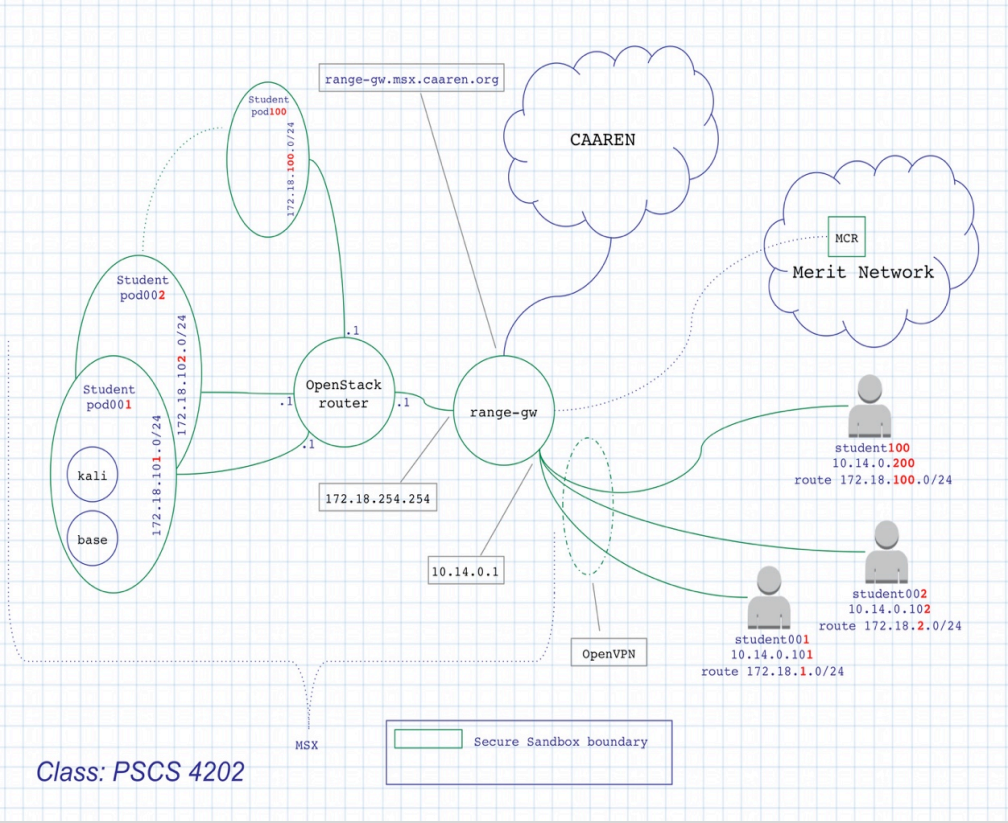
Course Learning Objectives

Upon completion of this course, students will be able to:

- Think like an attacker;
- Assess targets like an attacker;
- Understand the underlying principles of attack tools and construct their own;
- Use available toolkits that implement the discussed concepts;
- Mitigate attacks;
- Gain hands-on experience in concepts discussed;
- Interact with others in groups or teams to accomplish a series of goals

Class Hands-on Environment

Each student has their own dedicated environment mimicking real world cyberinfrastructures



Industrial Control and IoT Training and Testing

Real physical SCADA/IoT devices

- Siemens PLC
- IoT sensors
- virtual – physical integration

Industrial Control Systems, IoT

- actuation
- attacks
- pen testing
- benchmarking